

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**Applicant:** Steven J. Winick**Examiner:** Christian A. Laforgia**Serial No.:** 10/805,702**Art Unit:** 2139**Filed:** March 22, 2004**Docket:** H0006502-0555(17268)**For:** SUPERVISION OF HIGH VALUE
ASSETS**Conf. No.:** 8726

Commissioner for Patents
P.O. Box 1450
Alexandria, VA. 22313-1450

DECLARATION UNDER 37 C.F.R. §1.131

Sir:

I, **Steven J. Winick**, hereby declare that:

1. I am the Applicant in U.S. Patent Application No. 10/805,702 filed on March 22, 2004.
2. I conceived the invention that is disclosed and claimed in the present Application, prior to November 13, 2003. November 13, 2003 is the priority date of U.S. Patent Application 2007/0118645 to Suters, hereinafter "Suters," the reference cited against the present Application in the Office Action dated July 21, 2008.
3. As evidence of conception of the present invention prior to the effective filing date of Suters, attached hereto is Exhibit A, consisting of a redacted Invention Disclosure Form (IDF) submitted in order to initiate the patent application process.
4. Exhibit A evidences a conception of the claimed invention in Syosset, New York, prior to the November 13, 2003 effective filing date of Suters. The activity

contributing to this conception was conducted by me prior to the effective filing date of Suters.

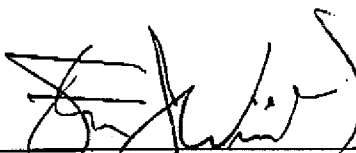
5. Exhibit A is believed to fully support the subject matter recited in claims 1, 10, and 28. Specifically, Exhibit A discloses, in sections 2 and 3, a device receiving a polling signal from a security system via a connection point, responding to the security system as an encrypted message, including a unique address / identifier to verify installation in an authorized network, and configuring the device as a security feature of the security system.
6. I exercised due diligence between said conception until the filing of the present Application on March 22, 2004.
7. Between the submission date of the IDF and November 14, 2003, the invention disclosure went through a standard approval process, wherein a committee reviews all invention disclosures to determine which invention disclosures are approved for filing.
8. On November 14, 2003, the assignee of the present application submitted the invention disclosure to outside counsel for preparation of the United States Patent Application No. 10/805,702. Annexed hereto and made a part of this Declaration is Exhibit B, an email from in-house counsel to outside counsel.
9. Between November 14, 2003, and March 8, 2004, outside counsel conferred with the Applicant via a series of e-mails and telephone conferences to prepare and file the present application.

10. Outside counsel submitted a proposed outline of the present Application on December 17, 2003. Attached hereto and made a part of this Declaration is Exhibit C, an email from outside counsel sending a proposed outline to the Applicant.
11. A first draft of the present application was sent for Applicant's review on January 29, 2004. Attached hereto and made a part of this Declaration is Exhibit D, an email enclosing a draft of the present application from outside counsel to Applicant.
12. After a thorough review of the draft, Applicant responded with comments and suggestions to improve the draft application. Attached hereto and made a part of this Declaration is Exhibit E, an email including Applicant's comments sent to outside counsel.
13. Outside counsel quickly responded with a revised draft on March 5, 2004. Attached hereto and made a part of this Declaration is Exhibit F, an email from outside counsel to Applicant enclosing the revised draft per Applicant's comments.
14. U.S. Patent Application 10/805,702 was filed on March 22, 2004, after a timely and expedient review of the final draft by the Applicant.

15. I further declare that I am a citizen of the United States, and I am at least 21 years of age. All statements made herein of my knowledge are true, and all statements made on information and belief are believed to be true. These statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both under 18 U.S.C. §1001, and that such willful false statements may jeopardize the validity of the patent application or any patent issued thereon.

Dated:

10/23/08



Steven J. Winick

Address: 375 Yale Ave, Woodmere, NY 11598

**Honeywell CONFIDENTIAL
ATTORNEY-CLIENT PRIVILEGED****REDACTED****Invention Record
(Docket) No.:
H0006502**

Origin Date:

SBE: 0555 - Security Solutions

Attorney(s): Beninati, John -

File Location: SY - Syosset, NY

Title: supervision of high value assets

Inventor: winick, steven j

SSN: *****

Address:

County: us

Phone:

Fax:

Supervisor:

Citizenship:

1. Briefly describe the technical or commercial problem or need that this invention is intended to solve. a consumer (or business) purchases assets that want to be connected to the security system as monitored assets for both local (and central station) annunciation as well as world wide tracking should they leave their approved location. in conversation with a leading consumer electronics manufacturer, he was describing the fact that much of his high end electronics, eg, plasma displays, audio control servers, etc. in the near future will feature ethernet connectivity to the home lan for two purposes. first, to permit networking and entertainment content transfer among devices in the home and second, to communicate with a server of theirs to download new software or some remote programming. we were talking about ideas for a unified user display for control these devices as well as security.

2. Briefly describe how this invention solves the problem or meets the need. my idea is to add two more functions. first, enable the device to communicate directly with the control panel (via symphony for example) and be a new kind of sensor point, for example, as a UPnP point. polled regularly and programmable as to response if it is removed from the house lan. second, give it the same security keys that we use in alarmnet-i and let it securely communicate with alarmnet-i automatically. this would permit more security functionality, but, maybe even more valuable is that we'll know where it is (at least an IP address that is generally geographically traceable). if it's moved (stolen or otherwise) and plugged back in, we can monitor. it would mean a bad guy could steal something, but never plug it back in to the internet to get the rest of its functionality. interesting consumer value proposition that we can monitor the asset on the wall, tell if it's moved and tell where if it's reactivated

3. Describe how to make and use the invention. Please indicate which embodiment(s) are preferred and describe the best way known to you to practice the invention. Attach relevant documents. (If the invention is a device or process, please provide a drawing or flow chart.) (If you are unfamiliar with the contents and preparation of a patent application, please refer to the Guidelines for the Preparation of Invention Disclosures. add UPnP functionality to the panel or a gateway and a security object to the consumer device so that the panel can configure and bind to it. add alarmnet-i functionality to permit remote supervision and tracking

Document(s):

4(a). To the best of your recollection what is the earliest date on which the invention was conceived? Who conceived the invention? Attach documents which evidence the foregoing.

Conception Date:

Who conceived it?: steve winick

Document(s):

EXHIBIT A

Honeywell DAS-Teterboro: On-Line Invention Disclosure System

file:///C:/Documents%20and%20Settings/anna/Local%20Settings/Temp/H0006502.htm

4(b). Is there a non-inventor who witnessed the conception? If so, please identify him/her and attach any documents which evidence the witnessing.

yes

Witness Name:

First Practice Documents:

5(a). To the best of your recollection, what is the earliest date on which the invention was reduced to practice (i.e. made)? Who reduced the invention to practice. Attach documents which evidence the foregoing. If no reduction to practice, type "n/a".

First Practice Documents:

First Practice Date: Who reduced it to practice?:

5(b). Is there a non-inventor who corroborated the reduction to practice? If so, please identify him/her, the corroborating activity (i.e., over-the-shoulder corroboration or repeating the experiment), and the date of the activity. Attach documents which evidence the foregoing.

Non-inventor corroborator?:

First Corroborator

First Corroborator Phone:

no

Name:

First Practice

Corroboration Date:

First Practice Corroborator Activity:

Document(s) related to corroboration event:

5(c). For each example of the invention and each comparative example on which you intend to rely in the patent application, please indicate when the example was generated, who conducted the experiment and where this example is recorded (e.g., volume, page and author or laboratory notebook) and attach a copy of these records. If no example available, type "n/a".

Example(s):

Example Date:

Who conducted the experiment?:

Where is example recorded?:

6(a). Did this invention arise in a program that is funded in whole or part by the U.S. Government or another company, or any entity other than Honeywell?

No

6(b). If so, please identify the program (including government contract number, if applicable) and the entity sponsoring the program and provide a copy of any agreement between the parties concerning the program.

Outside Funding Program:

Contract Number (if applicable):

Outside Funding Entity:

Document(s) related to funding agreement:

7(a). To your knowledge, is this invention subject to any agreement between Honeywell and a third party (e.g., a secrecy agreement, license agreement, joint development agreement, etc.)?

no

7(b). If so, please identify the agreement and the other party and attach a copy of the agreement if one is available.

Third party agreement ID:

Third party name:

REDACTED

EXHIBIT A

Honeywell DAS-Totator: On-Line Invention Disclosure System

file:///C:/Documents and Settings/anna/Local Settings/Temp/H0006502.htm

Document(s) related to any third party agreement:

8. You have a duty to disclose to the U.S. Patent and Trademark Office all relevant prior art of which you are aware. Please list all such prior art (e.g., patents, publications, brochures, Honeywell and third-party products) known to you. If a prior art search has been conducted, it must be included. Briefly indicate how this invention is different from the prior art. See 1 and 2 above.

List of prior art:

none

How invention is different from the prior art:

9(a). Has the product or process which is the subject of this invention disclosure been disclosed, sold or offered for sale to anyone outside of Honeywell or to the general public.

yes

9(b). If so, when and to whom was it disclosed, sold or offered for sale? If it was disclosed, was a secrecy agreement in place? Attach documents which evidence the sale or offer for sale.

Date it was disclosed

Whom disclosed to:

Disclosure Sales Agreement?:

Document(s) which evidence the sale or offer for sale:

9(c). Does the business intend to disclose, sell or offer to sell the invention to anyone outside of Honeywell or to the general public in the near future? If so, to whom and when is this disclosure, sale or offer for sale planned?

no

For whom are future sales planned:

Date future sale is planned:

10(a). Does this invention relate to any other: (i) issued patents, (ii) pending patent applications, or (iii) previously submitted invention disclosures, of Honeywell?

yes

10(b). If so, please identify the related matter and indicate whether this is an improvement on an earlier invention: Other patents related matter is:

alarmnet-i and symphony patents

Is this an improvement?:

no

11. Please specify the product(s) to which this invention disclosure relates.

security control panels. alarmnet-i services

12. Please indicate keywords for identifying this invention disclosure.

asset tracking supervision

REDACTED

EXHIBIT B

REDACTED

From:
To:
Date: 11/14/03 3:29PM
Subject: New Invention Disclosures for Filing

Paul,

Attached are four invention disclosures that were approved for filing at our last patent committee meeting. Please confirm that you can file the applications within Honeywell's budget constraints or per case and give approximate time when you can file.

I have attached:

I, H0006502, I and I

New requirements by Honeywell corporate are to include a dash and SBE number after each docket number. Therefore, please add a -0555 after each number. (Example H0006490-0555).

Thank you.

Regards,

Honeywell ACS, Intellectual Property
516-921-6704 X3098 FAX: 516-496-7374

CC:

From:
To: Steve_winick@ademco.com
Date: 12/17/03 4:01PM
Subject: Re: New US patent application

REDACTED

Re: New US patent application
Title: supervision of high value assets
Honeywell Ref.: H006502-0555 - My Ref.: 17268
Inventor: Steven J. Winick

Hi Steve,

I have been assigned to prepare the above-mentioned patent application. I have read the enclosed invention disclosure and have prepared the enclosed figure that perhaps we can use as a starting point.

My understanding is that a modern home network can include devices such as a plasma display and an audio control server that are connected in a LAN such as using Ethernet. As you indicated, this connection permits networking and content transfer among the devices. Additionally, the devices can communicate with a server ("server for devices") to receive data such as programming commands or new software downloads, and perhaps to send data such as diagnostic data.

Furthermore, using a system such as Ademco's AlarmNet-I system, a home security system may report alarms via the Internet (or an intranet, such as for a business). In this case, an alarm tx/rx module (such as the 7845I Internet Communicator or Symphony display) is provided that connects to a hub in the home that is used for home networking (such as the Ethernet hub) to communicate with an alarm server. The alarm server authenticates the alarm from the home before reporting the alarm to the central alarm monitoring station. The alarm tx/rx module and the alarm server use an encryption and authentication protocol. The alarm tx/rx module is triggered based on a conventional alarm at the alarm control panel.

Another trend in proximity networks such as home networks is the Universal plug and play (UPnP) protocol that allows devices to communicate with one another. The devices communicate with a UPnP control point using TCP/IP. The UPnP control point can be an operator's station or another device. A network supervisor can communicate with the UPnP network to determine the status of the devices, and which devices are running. The control points can also be notified of events of the devices.

The invention involves connecting the Ethernet-enabled devices to the Internet alarm reporting capability of the home security system. In one possible approach this is achieved by adding a UPnP capability to the devices and the home security system. (In my figure I show the UPnP hub communicating with the alarm control panel).

Also, the UPnP-enabled devices can use the same encryption scheme used by the security system for the Internet alarm reporting.

Please comment on this explanation. Also please explain further:

- how one would add the UPnP functionality to the panel or a gateway
- how to add a security object to the consumer device so that the panel can configure and bind to it
- how to add alarmnet-I functionality to permit remote supervision and tracking.

Thanks,

From:
To: Steve_winick@ademco.com
Date: 1/29/04 11:45AM
Subject: draft pat. app.

REDACTED

Re: New US patent application
Title: Supervision of High Value Assets
Honeywell Ref.: H006502-0555 - My Ref.: 17268
Inventor: Steven J. Winick

Steve,

The draft application is enclosed in this matter. Please review and comment.

Thanks,

This electronic message and attachments, if any, are intended only for the individual or entity named above or those properly entitled to access the information and may contain information that is privileged, confidential, attorney-work product or otherwise exempt from disclosure under applicable law. If the reader of this transmission is not the intended or an authorized recipient, you are hereby notified that any unauthorized distribution, dissemination, or copying of this transmission, is prohibited

If you have received this transmission in error, please contact the sender immediately and delete and destroy all copies of this transmission.

REDACTED

From: <Steve_Winick@Ademco.com>
To:
Date: 3/4/04 7:48PM
Subject: RE: draft app. revised version

you're right. It basically looks pretty good. here are a few comments:

typos in [0037] UpNP should be UPnP. UpnP should be UPnP

[0032] may want to refer to AlarmNet-I from Honeywell as an example of a server structure since this invention is really an extension of that idea

claims:

I'd add some more dependents related to encryption and authentication, both locally and to the server. the elements are that each device (145, 150) can have a pre-programmed, secret encryption code, which can be individually unique. in communication with the server, special pre-determined data is sent encrypted by that key with a selected encryption algorithm. the mating key is in the server. the server can look up the key, decrypt and thereby authenticate that the source of the message is genuine. ie, a bad guy didn't steal the plasma and leave a little \$30 box plugged in spoofing the security system with poll messages. same security for local poll / responses.

all communications with the server is initiated automatically by the device itself. this means that communications sessions can freely pass through local firewalls whereas server initiated communications attempts would be blocked by a premise firewall. for security, this means we don't have to know where (or what the device's IP) is in order to supervise it. it always, automatically initiates contact as soon as its plugged in. in the control sense, it means that we can control the device remotely if we choose to by waiting for it to initiate contact with us and then capture the TCP session and do whatever we wish. systems that attempt to use server initiated control fail to penetrate firewalls (or have to have an IT guy open a hole in the local firewall), have to know the local IP addresses and can't deal with dynamic IP assignment that is common (via DHCP)

it

hope this helps

-----Original Message-----

REDACTED

From:
To: Steve_winick@ademco.com
Date: 3/5/04 2:48PM
Subject: 2nd draft

Re: New US patent application
Title: Supervision of High Value Assets
Honeywell Ref.: H006502-0555 - My Ref.: 17268
Inventor: Steven J. Winick

Steve,

Enclosed is the revised draft per your comments, with the changes shown.

Please let me know if you have any other comments on the draft. Otherwise we can call it finalized.

Thanks,

This electronic message and attachments, if any, are intended only for the individual or entity named above or those properly entitled to access the information and may contain information that is privileged, confidential, attorney-work product or otherwise exempt from disclosure under applicable law. If the reader of this transmission is not the intended or an authorized recipient, you are hereby notified that any unauthorized distribution, dissemination, or copying of this transmission, is prohibited

If you have received this transmission in error, please contact the sender immediately and delete and destroy all copies of this transmission.